一种基于密钥的受控最低有效位修改技术的稳健型量子水印算法 *

李　涛 [1a]，程振文 [1a†]，瞿治国 [1b, 2]

(1. 南京信息工程大学 a. 电子与信息工程学院; b. 计算机与软件学院，南京 210044; 2. 江苏省网络监控工程中心，南京 210044)

摘　要：如何更好地保护量子图像的版权，是量子水印技术的一个重要研究课题。基于对数极坐标的量子图像表示，提出了一种新颖的量子水印算法。根据通信双方共享一组密钥的值，发送方选择量子载体图像像素灰度值的高四位中的某一位作为受控位；再根据所选受控位的值，发送方将水印信息嵌入到量子载体图像的最低有效位或次最低有效位上。这种基于密钥的受控最低有效位修改技术，提高了量子水印图像的透明性和稳健性。基于 MATLAB 的实验仿真和性能分析也表明新算法在透明性、稳健性和嵌入容量上有着良好的表现。

关键词：版权保护；量子水印技术；对数极坐标量子图像；最低有效位修改技术；透明性；稳健性；嵌入容量

中图分类号：TP309.2　　doi: 10.3969/j.issn.1001-3695.2018.05.0317

Robust quantum watermarking algorithm based on key to implement controlled least significant qubit modification technique

Li Tao[1a], Cheng Zhenwen[1a†], Qu Zhiguo[1b, 2]

(1. *a. School of Electronic & Information Engineering, b. School of Computer & Software, Nanjing University of Information Science & Technology, Nanjing* 210044, *China*; 2. *Jiangsu Engineering Center of Network Monitoring, Nanjing* 210044, *China*)

Abstract: How to better protect the copyright of quantum images is an important research subject in quantum watermarking technology. Based on the representation of quantum log-polar images, this paper proposed a novel quantum watermarking algorithm. According to the value of the key shared by the both communicating parties, the sender selected one of the high four qubits of the pixel gray value of quantum carrier image as the controlled qubit. And the watermarking information was embedded into the least significant qubit or the peripheral least significant qubit of quantum carrier image on the basis of the value of the selected controlled qubit. Utilizing the key to implement the controlled least significant qubit modification technique improved the transparency and robustness of quantum watermark image. Experimental simulation and performance analysis based on MATLAB showed that the new algorithm has a good performance on transparency, robustness and the embedding capacity.

Key words: copyright protection; quantum watermarking technology; quantum log-polar images; least significant qubit modification technique; transparency; robustness; embedding capacity

0　引言

作为一种崭新的计算模型，量子计算可以利用量子力学[1]的特殊性质，如叠加态和纠缠态来存储、处理和传输信息。近些年来，随着量子计算的快速发展和数字图像的广泛应用，为了满足采用量子态来存储数字图像的需求，多种量子图像表示模型被提出，如 Qubit Lattice[2]、Entangled Image[3]、Real Ket[4]、FRQI[5]、NEQR[6]、QUALPI[7]和 NCQI[8]等。其中，QUALPI 是基于对数极坐标的量子图像表示模型，具有旋转和缩放的不变性特点[9]。QUALPI 量子图像的三种变换，即对称变换、旋转变换和缩放变换，可以灵活快速地进行。

多种量子图像表示模型的提出，使得量子图像在通信网络中有着广阔的应用前景。基于不同量子图像表示模型的特点，量子图像隐写技术[10~12]和量子水印技术[13~16]也相应地被提

收稿日期：2018-05-30；**修回日期**：2018-07-11　　**基金项目**：国家自然科学基金资助项目（61373131，61303039，61232016，61501247）；公益性行业（气象）科研专项项目（GYHY201306070）；江苏高校品牌专业建设工程资助项目（PPZY2015B134）；江苏省高等学校大学生创新创业训练计划项目（201610300031）；南京信息工程大学江苏省大气环境与装备技术协同创新中心（CICAEET）资助项目；江苏高校优势学科建设工程资助项目（PAPD）

作者简介：李涛（1978-），男，副教授，博士，主要研究方向为数据挖掘、机器学习等；程振文（1992-），男（通信作者），硕士，主要研究方向为量子信息隐藏（ChengZhenwen_hb@163.com）；瞿治国（1976-），男，讲师，博士，主要研究方向为量子隐写、量子密码通信等.

出。相比于量子图像隐写技术侧重秘密信息在量子图像中的隐蔽性，量子水印技术则在量子图像的版权保护方面起到了至关重要的作用。量子水印技术是将标志信息（即量子水印）嵌入到量子载体（包括文本、图像、视频等）当中，既不影响量子载体的使用价值，也不轻易让非法第三方察觉到量子水印的存在。通过这些隐藏在量子载体中的水印信息，可以达到版权保护的目的。目前，量子水印技术取得的主要研究成果如下所述。

2013 年，Zhang 等人[13]提出了一种通用的量子水印算法，可以根据提取出的水印找出真正的水印嵌入者，而且任何非版权所有者都无法去除嵌入的水印。同一年，一种基于量子傅里叶变换（QFT）的量子水印算法也被 Zhang 等人[14]提出。该算法将量子水印图像的信息嵌入到量子载体图像的傅里叶系数中，利用傅里叶变换的性质，确保含水印的量子载体图像能够抵抗无法避免的噪声。2016 年，运用经典的最低有效位（LSB[17]）修改技术的思想，Sang 等人[15]首先给出了量子的最低有效位（LSQb）修改技术的思想，接着提出基于量子彩色图像表示模型（NCQI）的量子水印算法，使得该算法具有易操作和信息隐藏量大等优点。

透明性、稳健性以及嵌入容量是评估量子水印算法性能的三个重要指标。其中稳健性是评估量子水印算法的关键。任何一种量子水印算法的提出，只有经得住非法第三方各种攻击的考验才是安全的，一旦误用弱稳健性的量子水印算法，可能使合法的版权所有者的利益受到损失。若非法第三方试图删除或者破坏图像中存在的水印，则会导致载体图像存在严重失真，这种恶意攻击也使得非法第三方无法获取水印信息。若非法第三方采用扫描与复印、几何变换和噪声污染等攻击，不仅对载体图像造成的影响较小，而且非法第三方还会获取一部分水印信息。这种无意攻击通常是非法第三方采用的攻击手段。上述三种量子水印算法着重分析了扫描与复印和噪声污染这两种攻击对算法的影响，但却忽略了几何变换攻击对含水印的量子载体图像的影响。因此，提出一种能有效抵抗几何变换攻击的稳健型量子水印算法，具有重要的现实意义。

针对这方面的需求，Qu 等人[16]在 2017 年提出了一种基于 QUALPI 量子图像的稳健型量子水印算法。该算法将量子水印图像以 LSQb 修改技术的方式嵌入到量子载体图像中，再利用 QUALPI 量子图像具有旋转和缩放的不变性特点，使得含水印的量子载体图像能有效抵抗旋转、翻转和缩放等常见的几何变换攻击，具有良好的稳健性。虽然该算法利用 LSQb 修改技术易操作的优点，但是当非法第三方获取到含水印的量子载体图像，并从中读取出最低比特位平面时，非法第三方仍然有很大几率得知水印信息，使得该算法存在安全性隐患。1984 年，Bennett 等人[18]提出了第一个量子密钥分发协议，即 BB84 协议，达到让合法通信者共享一串随机密钥的目的，并且非法第三方不能得到关于密钥的任何信息。因此，本文提出了一种基于密钥的受控最低有效位修改技术的稳健型量子水印算法。即使非法第三方获取到含水印的量子载体图像，由于不知道密钥信息，所以无法得知水印信息，进一步提高了算法的稳健性。

1 基于对数极坐标的量子图像表示模型

假设对数极坐标数字图像的对数半径 ρ 和角方向 θ 的采样分辨率分别为 2^m 和 2^n，那么基于对数极坐标的量子图像表示模型（QUALPI），该数字图像可以表示为

$$|F\rangle = \frac{1}{\sqrt{2^{m+n}}} \sum_{\rho=0}^{2^m-1} \sum_{\theta=0}^{2^n-1} \left(|G(\rho,\theta)\rangle \otimes |\rho\rangle \otimes |\theta\rangle \right) \tag{1}$$

其中：$G(\rho,\theta)$ 表示第 $\rho\theta$ 个像素的灰度值。若数字图像的灰度范围是 2^q，则像素的灰度值可以用二进制序列 $g_{q-1}g_{q-2}\cdots g_1 g_0$ 编码，即

$$G(\rho,\theta) = g_{q-1}g_{q-2}\cdots g_1 g_0, G(\rho,\theta) \in \left[0, 2^q - 1\right] \tag{2}$$

相应的，对数半径 ρ 和角方向 θ 也可编码为

$$|\rho\rangle \otimes |\theta\rangle = |\rho_{m-1}\rho_{m-2}\cdots\rho_0\rangle \otimes |\theta_{n-1}\theta_{n-2}\cdots\theta_0\rangle \tag{3}$$

式（1）表明，整个 QUALPI 量子图像存储在一个归一化和等概率的量子叠加态中，每个基态表示一个像素。基态由三个量子比特序列的张量积组成，像素的所有信息，包括灰度值、对数半径和角方向，都存储在基态中。

图 1 是一幅大小为 2×4、灰度范围为 256 的 QUALPI 量子图像的示例。采用 QUALPI 模型可以表示为

$$\begin{aligned} |F\rangle = \frac{1}{2\sqrt{2}} \Big[& |00001111\rangle \otimes \left(|000\rangle + |001\rangle + |010\rangle + |011\rangle \right) \\ & + |11110000\rangle \otimes \left(|100\rangle + |101\rangle + |110\rangle + |111\rangle \right) \Big] \end{aligned} \tag{4}$$

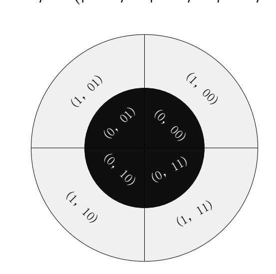


图 1 QUALPI 量子图像的示例

2 量子水印算法

运用基于密钥的受控最低有效位（LSQb）修改技术，本文提出了一种新颖的量子水印算法。新算法由量子水印图像的嵌入过程和提取过程两部分组成。其流程如图 2 所示。

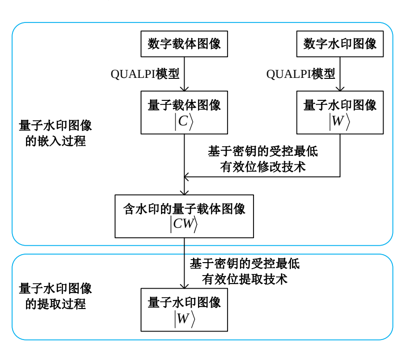


图 2 新颖的量子水印算法的流程

2.1　量子水印图像的嵌入过程

量子水印图像的嵌入过程如下所述。

a)假设数字载体图像是一幅大小为 $2^m \times 2^n$ 的灰度图像，数字水印图像是一幅大小为 $2^m \times 2^n$ 的二值图像。制备基于 QUALPI 模型的量子载体图像 $|C\rangle$ 和量子水印图像 $|W\rangle$，其表达式分别如式（5）和（6）所示。

$$|C\rangle = \frac{1}{\sqrt{2^{m+n}}}\sum_{\rho=0}^{2^m-1}\sum_{\theta=0}^{2^n-1}|c_7c_6\cdots c_1c_0\rangle|\rho\theta\rangle \tag{5}$$

$$|W\rangle = \frac{1}{\sqrt{2^{m+n}}}\sum_{\rho=0}^{2^m-1}\sum_{\theta=0}^{2^n-1}|w_0\rangle|\rho\theta\rangle \tag{6}$$

b)发送方和接收方共享一组密钥 K：

$$K = k_0k_1\cdots k_{2t}k_{2t+1}\cdots k_{2(2^{m+n}-1)}k_{2(2^{m+n}-1)+1}, t\in\left[0,2^{m+n}-1\right] \tag{7}$$

其中 t 的值对应于量子载体图像 $|C\rangle$ 第 ji 个像素。

根据密钥 $k_{2t}k_{2t+1}$ 的值，发送方将选择量子载体图像 $|C\rangle$ 第 ji 个像素灰度值 $\left|c_7^{ji}c_6^{ji}c_5^{ji}c_4^{ji}c_3^{ji}c_2^{ji}c_1^{ji}c_0^{ji}\right\rangle$ 的高四位中的某一位作为控制位，规定：

如果 $k_{2t}k_{2t+1}$=00，选择 $\left|c_7^{ji}\right\rangle$ 作为控制位；

如果 $k_{2t}k_{2t+1}$=01，选择 $\left|c_6^{ji}\right\rangle$ 作为控制位；

如果 $k_{2t}k_{2t+1}$=10，选择 $\left|c_5^{ji}\right\rangle$ 作为控制位；

如果 $k_{2t}k_{2t+1}$=11，选择 $\left|c_4^{ji}\right\rangle$ 作为控制位。

再根据所选控制位的值，发送方将量子水印图像 $|W\rangle$ 第 ji 个像素灰度值 $\left|w_0^{ji}\right\rangle$ 嵌入到最低有效位 $\left|c_0^{ji}\right\rangle$ 或次最低有效位 $\left|c_1^{ji}\right\rangle$ 上，即

（a）如果控制位是 $|0\rangle$，那么将 $\left|w_0^{ji}\right\rangle$ 嵌入到最低有效位 $\left|c_0^{ji}\right\rangle$ 上。具体的酉操作为：

如果 $\left|w_0^{ji}\right\rangle$ 和 $\left|c_0^{ji}\right\rangle$ 相同，那么不翻转 $\left|c_0^{ji}\right\rangle$ 的值。定义酉变换 U_S^{ji}：

$$U_S^{ji} = I^{\otimes 8}\otimes\left(\sum_{\rho=0}^{2^m-1}\sum_{\theta=0}^{2^n-1}|\rho\theta\rangle\langle\rho\theta|\right) \tag{8}$$

其中：I 表示 Pauli 矩阵 σ_I：

$$I = \sigma_I = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \tag{9}$$

此时，酉变换 U_S^{ji} 作用在量子载体图像 $|C\rangle$ 上，有

$$\begin{aligned}U_S^{ji}(|C\rangle) &= \left(I^{\otimes 8}\otimes\sum_{\rho=0}^{2^m-1}\sum_{\theta=0}^{2^n-1}|\rho\theta\rangle\langle\rho\theta|\right)\\ &\left(\frac{1}{\sqrt{2^{m+n}}}\sum_{\rho=0}^{2^m-1}\sum_{\theta=0}^{2^n-1}|c_7c_6\cdots c_1c_0\rangle|\rho\theta\rangle\right)\\ &= \frac{1}{\sqrt{2^{m+n}}}\sum_{\rho=0}^{2^m-1}\sum_{\theta=0}^{2^n-1}|c_7c_6\cdots c_1c_0\rangle|\rho\theta\rangle\end{aligned} \tag{10}$$

如果 $\left|w_0^{ji}\right\rangle$ 和 $\left|c_0^{ji}\right\rangle$ 不相同，那么翻转 $\left|c_0^{ji}\right\rangle$ 的值。定义酉变换 U_D^{ji}：

$$U_D^{ji} = I^{\otimes 7}\otimes X\otimes|ji\rangle\langle ji| + I^{\otimes 8}\otimes\left(\sum_{\rho=0}^{2^m-1}\sum_{\theta=0,\rho\theta\neq ji}^{2^n-1}|\rho\theta\rangle\langle\rho\theta|\right) \tag{11}$$

其中：X 表示 Pauli 矩阵 σ_X 。

$$X = \sigma_X = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} \tag{12}$$

此时，酉变换 U_D^{ji} 作用在量子载体图像 $|C\rangle$ 上，有

$$\begin{aligned}U_D^{ji}(|C\rangle) &= \left(I^{\otimes 7}\otimes X\otimes|ji\rangle\langle ji| + I^{\otimes 8}\otimes\sum_{\rho=0}^{2^m-1}\sum_{\theta=0,\rho\theta\neq ji}^{2^n-1}|\rho\theta\rangle\langle\rho\theta|\right)\\ &\left(\frac{1}{\sqrt{2^{m+n}}}\sum_{\rho=0}^{2^m-1}\sum_{\theta=0}^{2^n-1}|c_7c_6\cdots c_1c_0\rangle|\rho\theta\rangle\right)\\ &= \frac{1}{\sqrt{2^{m+n}}}\left(I^{\otimes 7}\otimes X\otimes|ji\rangle\langle ji| + I^{\otimes 8}\otimes\sum_{\rho=0}^{2^m-1}\sum_{\theta=0,\rho\theta\neq ji}^{2^n-1}|\rho\theta\rangle\langle\rho\theta|\right)\\ &\left(\left|c_7^{ji}c_6^{ji}\cdots c_1^{ji}c_0^{ji}\right\rangle|ji\rangle + \sum_{\rho=0}^{2^m-1}\sum_{\theta=0,\rho\theta\neq ji}^{2^n-1}|c_7c_6\cdots c_1c_0\rangle|\rho\theta\rangle\right)\\ &= \frac{1}{\sqrt{2^{m+n}}}\left(\left|c_7^{ji}c_6^{ji}\cdots c_1^{ji}\bar{c}_0^{ji}\right\rangle|ji\rangle + \sum_{\rho=0}^{2^m-1}\sum_{\theta=0,\rho\theta\neq ji}^{2^n-1}|c_7c_6\cdots c_1c_0\rangle|\rho\theta\rangle\right)\end{aligned} \tag{13}$$

其中 $\left|\bar{c}_0^{ji}\right\rangle$ 是 $\left|c_0^{ji}\right\rangle$ 的相反状态，即

$$\left|\bar{c}_0^{ji}\right\rangle = \begin{cases}|0\rangle, \left|c_0^{ji}\right\rangle = |1\rangle\\ |1\rangle, \left|c_0^{ji}\right\rangle = |0\rangle\end{cases} \tag{14}$$

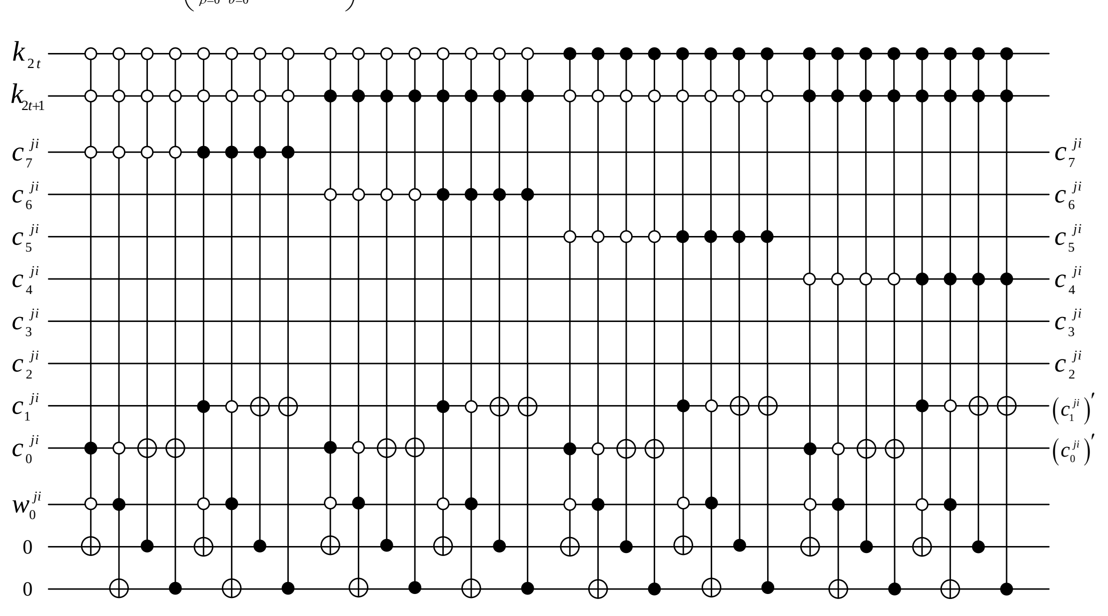


图 3　基于密钥的受控 LSQb 修改技术的量子线路

通过酉变换 U_S^{ji} 或者 U_D^{ji}，就可以将 $|w_0^{ji}\rangle$ 嵌入到 $|c_0^{ji}\rangle$ 上。

（b）如果控制位是 $|1\rangle$，那么将 $|w_0^{ji}\rangle$ 嵌入到次最低有效位 $|c_1^{ji}\rangle$ 上。定义两种酉变换 V_S^{ji} 和 V_D^{ji}：

$$V_S^{ji} = I^{\otimes 8} \otimes \left(\sum_{\rho=0}^{2^m-1}\sum_{\theta=0}^{2^n-1}|\rho\theta\rangle\langle\rho\theta|\right) \tag{15}$$

$$V_D^{ji} = I^{\otimes 6}\otimes X\otimes I\otimes|ji\rangle\langle ji| + I^{\otimes 8}\otimes\left(\sum_{\rho=0}^{2^m-1}\sum_{\theta=0,\rho\theta\neq ji}^{2^n-1}|\rho\theta\rangle\langle\rho\theta|\right) \tag{16}$$

如果 $|w_0^{ji}\rangle$ 和 $|c_1^{ji}\rangle$ 相同，那么酉变换 V_S^{ji} 作用在量子载体图像 $|C\rangle$ 上，有

$$\begin{aligned} V_S^{ji}\left(|C\rangle\right) &= \left(I^{\otimes 8}\otimes\sum_{\rho=0}^{2^m-1}\sum_{\theta=0}^{2^n-1}|\rho\theta\rangle\langle\rho\theta|\right) \\ &\quad\left(\frac{1}{\sqrt{2^{m+n}}}\sum_{\rho=0}^{2^m-1}\sum_{\theta=0}^{2^n-1}|c_7c_6\cdots c_1c_0\rangle|\rho\theta\rangle\right) \\ &= \frac{1}{\sqrt{2^{m+n}}}\sum_{\rho=0}^{2^m-1}\sum_{\theta=0}^{2^n-1}|c_7c_6\cdots c_1c_0\rangle|\rho\theta\rangle \end{aligned} \tag{17}$$

如果 $|w_0^{ji}\rangle$ 和 $|c_1^{ji}\rangle$ 不相同，那么酉变换 V_D^{ji} 作用在量子载体图像 $|C\rangle$ 上，有

$$\begin{aligned} V_D^{ji}\left(|C\rangle\right) &= \left(I^{\otimes 6}\otimes X\otimes I\otimes|ji\rangle\langle ji| + I^{\otimes 8}\otimes\sum_{\rho=0}^{2^m-1}\sum_{\theta=0,\rho\theta\neq ji}^{2^n-1}|\rho\theta\rangle\langle\rho\theta|\right) \\ &\quad\left(\frac{1}{\sqrt{2^{m+n}}}\sum_{\rho=0}^{2^m-1}\sum_{\theta=0}^{2^n-1}|c_7c_6\cdots c_1c_0\rangle|\rho\theta\rangle\right) \\ &= \frac{1}{\sqrt{2^{m+n}}}\left(I^{\otimes 6}\otimes X\otimes I\otimes|ji\rangle\langle ji| + I^{\otimes 8}\otimes\sum_{\rho=0}^{2^m-1}\sum_{\theta=0,\rho\theta\neq ji}^{2^n-1}|\rho\theta\rangle\langle\rho\theta|\right) \\ &\quad\left(|c_7^{ji}c_6^{ji}\cdots c_1^{ji}c_0^{ji}\rangle|ji\rangle + \sum_{\rho=0}^{2^m-1}\sum_{\theta=0,\rho\theta\neq ji}^{2^n-1}|c_7c_6\cdots c_1c_0\rangle|\rho\theta\rangle\right) \\ &= \frac{1}{\sqrt{2^{m+n}}}\left(|c_7^{ji}c_6^{ji}\cdots \bar{c}_1^{ji}c_0^{ji}\rangle|ji\rangle + \sum_{\rho=0}^{2^m-1}\sum_{\theta=0,\rho\theta\neq ji}^{2^n-1}|c_7c_6\cdots c_1c_0\rangle|\rho\theta\rangle\right) \end{aligned} \tag{18}$$

通过酉变换 V_S^{ji} 或者 V_D^{ji}，就可以将 $|w_0^{ji}\rangle$ 嵌入到 $|c_1^{ji}\rangle$ 上。

这种基于密钥的受控 LSQb 修改技术的嵌入方法，可由图 3 设计的量子线路来实现。在图 3 中，符号“•”“ο”和“⊕”分别代表 1 控制位、0 控制位和受控非门，并且常数输入量子比特 $|0\rangle$ 是辅助量子比特。为了方便起见，基于密钥的受控 LSQb 修改技术的量子线路方块图省略了辅助输入和无关输出，如图 4 所示。

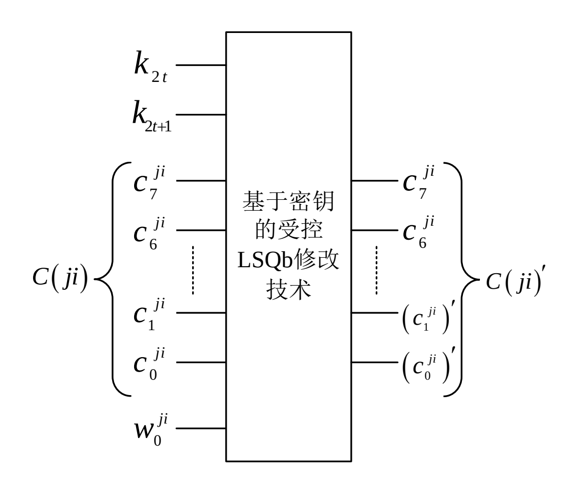


图 4　基于密钥的受控 LSQb 修改技术的量子线路方块图

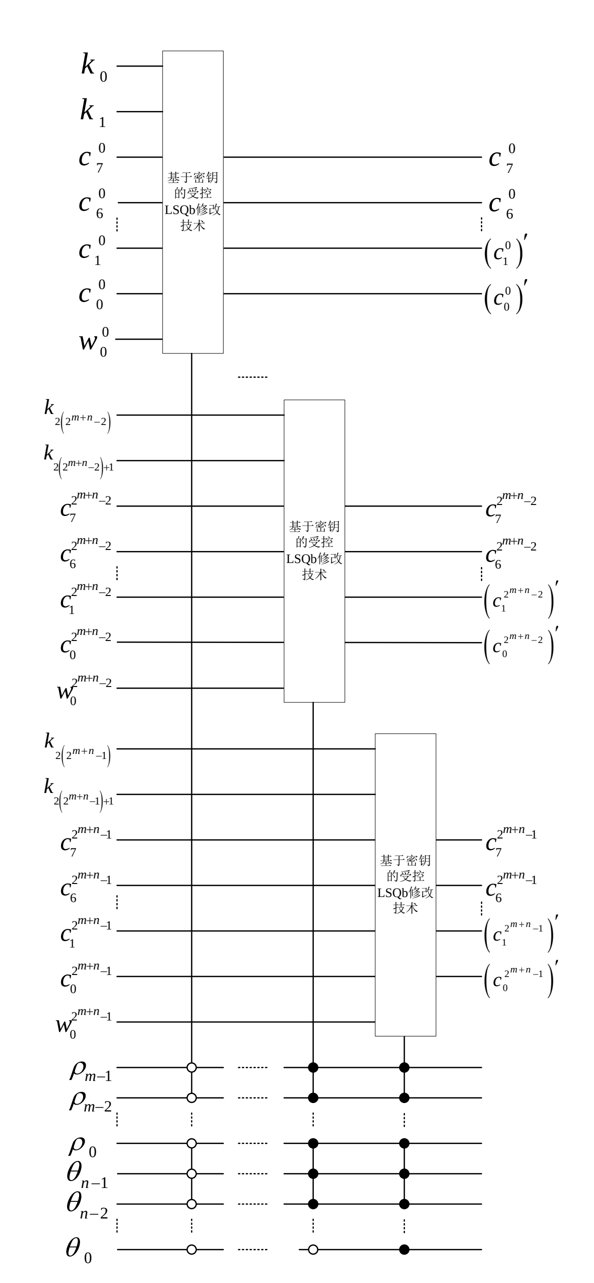


图 5　量子水印图像的嵌入量子线路

c)通过执行 2^{m+n} 次 b)，量子水印图像 $|W\rangle$ 的所有信息就会嵌入到量子载体图像 $|C\rangle$ 中，得到含水印的量子载体图像 $|CW\rangle$：

$$|CW\rangle = \frac{1}{\sqrt{2^{m+n}}}\sum_{\rho=0}^{2^m-1}\sum_{\theta=0}^{2^n-1}\left|c_7c_6\cdots(c_1)'(c_0)'\right\rangle|\rho\theta\rangle \tag{19}$$

为了提高新算法的可执行性，本文设计了一种高效的量子水印图像的嵌入量子线路，如图 5 所示。这种基于密钥的受控 LSQb 修改技术的嵌入方法，既保证了含水印的量子载体图像 $|CW\rangle$ 在视觉上与原始的量子载体图像 $|C\rangle$ 没有明显差别，也使得新算法具有良好的稳健性。

至此，量子水印图像的嵌入过程就完成了。

2.2　量子水印图像的提取过程

量子水印图像的提取过程如下所述。

a) 在希尔伯特空间中，含水印的量子载体图像 $|CW\rangle$ 是一个复杂的向量，需要把该向量分解成灰度值信息和像素位置信息的张量积形式。假设含水印的量子载体图像 $|CW\rangle$ 对应的矢量是 Q，则矢量 Q 可分解成如下形式：

$$Q = a_0 \otimes \begin{pmatrix}1\\0\\0\\\vdots\\0\\0\end{pmatrix} + \cdots + a_{2^{m+n}-2} \otimes \begin{pmatrix}0\\0\\0\\\vdots\\1\\0\end{pmatrix} + a_{2^{m+n}-1} \otimes \begin{pmatrix}0\\0\\0\\\vdots\\0\\1\end{pmatrix} \tag{20}$$

其中：符号“$\otimes$”表示张量积。张量积的第一部分和第二部分分别是含水印的量子载体图像$|CW\rangle$的灰度值信息和对应像素的位置信息。

b)为了提取水印信息，将灰度值信息 a_0、…、$a_{2^{m+n}-2}$ 和 $a_{2^{m+n}-1}$ 转换成相应的二进制码 b_0、…、$b_{2^{m+n}-2}$ 和 $b_{2^{m+n}-1}$。b_t 对应于含水印的量子载体图像$|CW\rangle$第 ji 个像素的灰度值：

$$b_t = \left|c_7^{ji}c_6^{ji}c_5^{ji}c_4^{ji}c_3^{ji}c_2^{ji}\left(c_1^{ji}\right)'\left(c_0^{ji}\right)'\right\rangle \tag{21}$$

c)根据密钥 $k_{2t}k_{2t+1}$ 的值，以及通信双方预先制定的规则，接收方从灰度值 b_t 的高四位中确定控制位。如果控制位是$|0\rangle$，那么灰度值 b_t 的最低有效位$\left|\left(c_0^{ji}\right)'\right\rangle$为水印信息；反之，次最低有效位$\left|\left(c_1^{ji}\right)'\right\rangle$为水印信息。这种基于密钥的受控 LSQb 提取技术的提取方法，可由图 6 设计的量子线路来实现。基于密钥的受控 LSQb 提取技术的量子线路方块图，如图 7 所示，则省略了无关输出。

本文也设计了一种高效的量子水印图像的提取量子线路，如图 8 所示。在图 8 中，2^{m+n} 个输入量子比特$|0\rangle$对应的输出量子比特，分别是量子水印图像$|W\rangle$每个像素的灰度值信息。

从上述步骤可知，量子水印图像的提取过程其实是嵌入过程的一个逆过程。

3　实验仿真结果和相关性能分析

评估量子水印算法性能主要有三个重要指标，分别是透明性、稳健性和嵌入容量。透明性要求嵌入在量子载体中的量子水印是不可知觉的，而且不影响量子载体的正常使用。稳健性是指在经历多种恶意攻击或无意攻击后，量子水印仍能保持部分完整性，并能准确鉴别。嵌入容量计算嵌入在量子载体中的量子水印的信息量。为了更好地分析本文所提出的量子水印算法在透明性、稳健性和嵌入容量上的性能，本章将给出若干新算法在经典计算机 MATLAB R2012a 环境下得到的实验数据。实验所用的载体灰度图像为 Girl、Woman、Lena 和 Vegetables，水印二值图像为 Thumbs-up、Recycling、Ribbon 和 Butterfly，分别如图 9 和 10 所示，其图像大小均为 256×256。

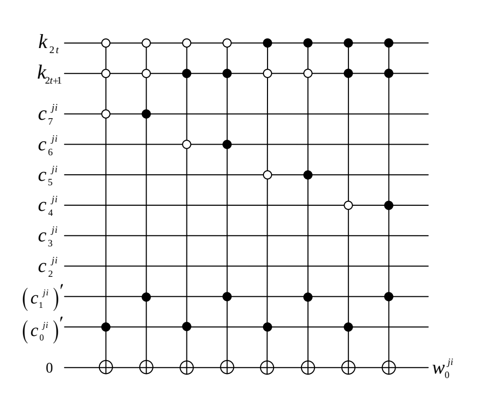


图 6　基于密钥的受控 LSQb 提取技术的量子线路

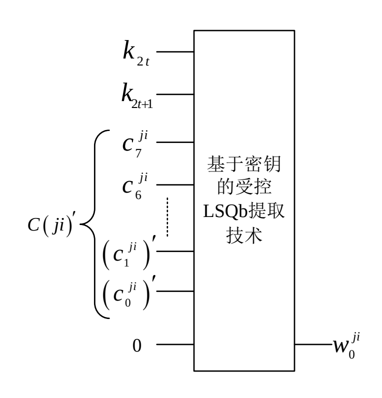


图 7　基于密钥的受控 LSQb 提取技术的量子线路方块图

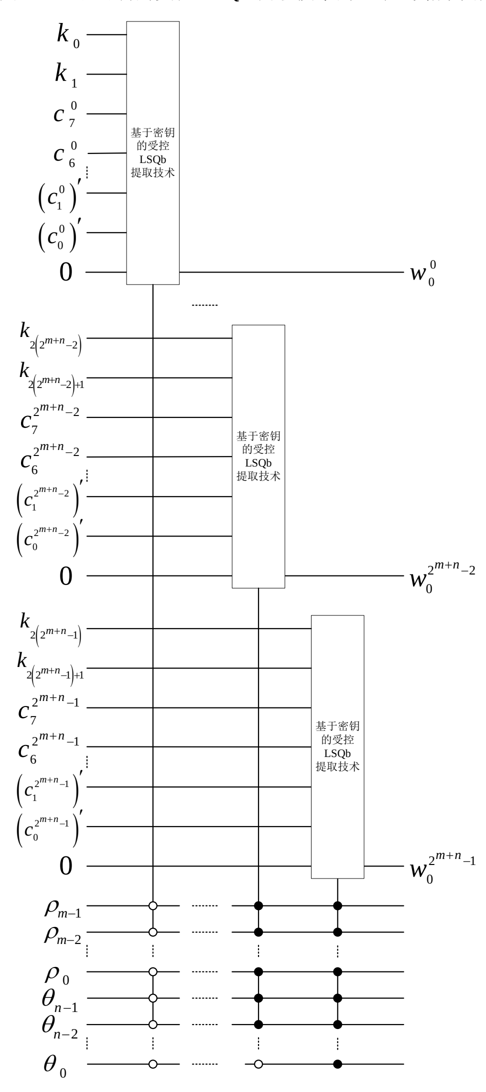


图 8　量子水印图像的提取量子线路



图 9　实验所用的载体灰度图像

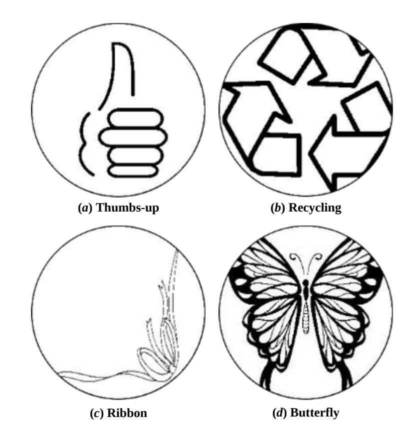


图 10　实验所用的水印二值图像

3.1　透明性

原始的量子载体图像与含水印的量子载体图像之间的保真度，是评估量子水印算法透明性最常用的方法。在经典数字图像处理中，峰值信噪比（PSNR）则是最广泛使用的评鉴画质的测量方法。假设 I 是原始的载体图像，J 是含水印的载体图像，式（22）和（23）分别给出了均方误差（MSE）和 PSNR 的计算公式。

$$MSE=\frac{1}{mn}\sum_{\rho=0}^{2^m-1}\sum_{\theta=0}^{2^n-1}\left[I(\rho,\theta)-J(\rho,\theta)\right]^2 \quad (22)$$

$$PSNR=20\log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \quad (23)$$

其中：$I(\rho,\theta)$ 和 $J(\rho,\theta)$ 分别表示原始的载体图像 I 和含水印的载体图像 J 在第 (ρ,θ) 个像素的灰度值；MAX_I 是原始的载体图像 I 的最大灰度值。

水印二值图像 Thumbs-up、Recycling、Ribbon 和 Butterfly，采用基于密钥的受控最低有效位修改技术的方法，分别嵌入到载体灰度图像 Girl、Woman、Lena 和 Vegetables 中，得到含水印的载体图像，如图 11 所示。在图 11 中，单靠人眼是无法有效区分原始的载体图像和含水印的载体图像。此外，计算图 11 中原始的载体图像与对应的含水印的载体图像之间的 PSNR 值，计算结果如表 1 所示。在表 1 中，PSNR 值都高于图像质量标准 38 dB，表明含水印的载体图像失真较小。因此，新算法具有良好的透明性。

3.2　稳健性

稳健性是评估量子水印算法的关键。嵌入在量子载体中的量子水印，不仅使非法第三方难以探知，也要使当非法第三方对含水印的量子载体进行攻击之后，量子水印受到的影响较小。非法第三方的攻击手段分为恶意攻击和无意攻击。恶意攻击（如数据窜改和有损压缩）有极大的几率删除，甚至破坏嵌入在量子载体中的量子水印，使得通信双方和非法第三方都无法获取量子水印。因而量子水印算法通常会着重分析非法第三方的无意攻击对量子水印的影响。常见的无意攻击有扫描与复印、几何变换和噪声污染等攻击。

为了保证所提出的量子水印算法在稳健性上有良好的表现，本节将从非法第三方的扫描与复印、几何变换和噪声污染这三种攻击来分析新算法的稳健性。



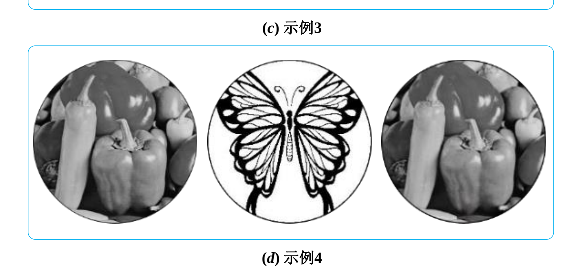


图 11　透明性的仿真结果

在四组示例中，每组示例的第一幅图是原始的载体图像，第二幅图是水印图像，第三幅图是含水印的载体图像

表 1　在图 11 中，原始的载体图像与对应的含水印的载体图像之间的 PSNR 值

水印图像	载体图像	PSNR/dB
Thumbs-up	Girl	44.7304
Recycling	Woman	46.1151
Ribbon	Lena	46.1146
Butterfly	Vegetables	46.1284

首先，根据量子水印图像的嵌入过程，分析扫描与复印攻

击对新算法的影响。当非法第三方对含水印的量子载体图像进行扫描与复印之后，非法第三方可以获取该图像像素信息的最低比特位平面和次最低比特位平面。非法第三方试图从这两个位平面中获取水印信息，这是徒然的。因为量子水印图像是以基于密钥的受控最低有效位修改技术的方式嵌入到量子载体图像中，而且通信双方共享的密钥是绝对安全的，所以非法第三方并不知道量子水印图像嵌入到量子载体图像中的具体位置。通信双方共享的密钥提高了新算法的稳健性。

接着，根据对数极坐标的量子图像表示模型（QUALPI）特性，分析几何变换攻击对新算法的影响。QUALPI 量子图像具有旋转和缩放的不变性特点，使得 QUALPI 量子图像的三种变换，即对称变换、旋转变换和缩放变换，可以灵活快速地进行。当非法第三方对含水印的量子载体图像进行几何变换攻击之后，接收方仍然可以通过酉变换恢复出原始的含水印的量子载体图像，并从中提取出量子水印图像。

为了证明上述论点，对图 11 中四组示例的含水印的载体图像分别进行旋转、水平轴翻转、垂直轴翻转和缩放等几何变换，仿真结果如图 12 所示。在图 12 中，受到几何变换攻击后的含水印的载体图像仍可恢复出含水印的载体图像。运用基于密钥的受控最低有效位提取技术的提取方法，从含水印的载体图像中提取出水印图像，仍具有很高的图像质量。采用 QUALPI 模型表示载体图像和水印图像也提高了新算法的稳健性。

最后，根据经典数字图像处理中另一个常用的误码率（BER），分析噪声污染攻击对新算法的影响。含水印的载体图像在通信网络中传输时，由于信道中存在着噪声，使得输出的图像产生误码，在某种程度上与原始的含水印的载体图像不一样。而单靠人眼是无法分辨出这两张图像的区别，因此，采用误码率来衡量噪声污染在图像传输过程中的影响。BER 定义为 PSNR 的倒数，即

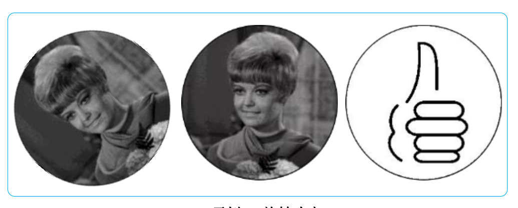
$$BER = {}^{1}\!/_{PSNR} \tag{24}$$

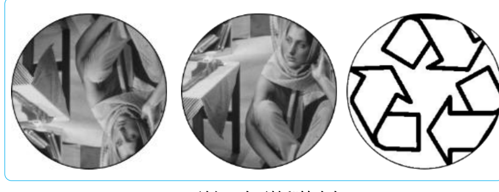
根据表 1 给出的 PSNR 值，计算得到 BER 值，如表 2 所示。在表 2 中，新算法的 BER 值都比较小，表明噪声污染对新算法的影响较小。

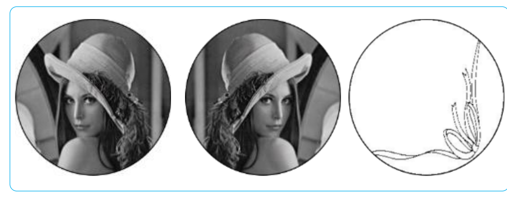
通过分析非法第三方的无意攻击，表明新算法具有良好的稳健性。

3.3　嵌入容量

量子水印算法的嵌入容量可由嵌入率和修改率来衡量。根据嵌入率的定义（嵌入率=嵌入水印的比特数/载体图像所有像素的个数），可知新算法的嵌入率为 1。此外，根据修改率的定义（修改率=载体图像单位像素被修改的比特数/嵌入水印的比特数），假定水印二值图像的 0 值比特和 1 值比特均匀分布，那么载体图像单位像素的最低有效位或次最低有效位，有 50% 的概率被修改，可知新算法的修改率为 0.5。


(a) 示例1：旋转攻击


(b) 示例2：水平轴翻转攻击


(c) 示例3：垂直轴翻转攻击


(d) 示例4：缩放攻击

图 12　稳健性仿真结果

在四组示例中，每组示例的第一幅图是受到几何变换攻击后的含水印的载体图像，第二幅图是通过酉变换恢复出的含水印的载体图像，第三幅图是提取出的水印图像

表 2　根据表 1 的 PSNR 值，计算得到 BER 值

水印图像	载体图像	BER
Thumbs-up	Girl	0.0224
Recycling	Woman	0.0217
Ribbon	Lena	0.0217
Butterfly	Vegetables	0.0217

4　结束语

运用对数极坐标的量子图像表示模型（QUALPI）具有旋转和缩放的不变性特点，以及基于密钥的受控最低有效位修改技术具有易操作的优点，本文提出了一种新颖的稳健型量子水印算法。相比于以往的量子水印算法，新算法利用 QUALPI 量子图像的特点，当含水印的量子载体图像受到旋转、翻转和缩放等几何变换攻击时，仍可从图像中提取出所嵌入的量子水印图像，保证了含水印的量子载体图像的稳健性。此外，基于密钥的受控最低有效位修改技术的嵌入方法，使得非法第三方在无法获取密钥信息的情况下，即便对含水印的量子载体图像进行扫描与复印攻击，也无法恢复出量子水印图像，进一步保护了量子图像的版权。

基于 MATLAB 给出的实验仿真，再结合经典数字图像处理中的峰值信噪比和误码率，对新算法的透明性和稳健性进行

分析。仿真结果和实验数据也表明新算法具有良好的透明性和稳健性。根据对新算法的嵌入容量进行分析，新算法的嵌入率为 1，这是一个比较可观的嵌入率。

本文另外一个创新之处是设计了基于密钥的受控最低有效位修改技术的量子线路和基于密钥的受控最低有效位提取技术的量子线路，一方面确保新算法在实现过程中严格遵循了量子力学原理，且在当前的物理实验条件下是可行的；另一方面也使得新算法具有很好的实用性。

参考文献：

[1] Nielsen M A, Chuang I L. Quantum computation and quantum information [J]. Cambridge University Press, 2011, 21 (1): 1-59.

[2] Venegas-Andraca S E, Bose S. Storing, processing and retrieving an image using quantum mechanics [J]. Quantum Information and Computation, 2003, 5105 (8): 1085-1090.

[3] Venegas-Andraca S E, Ball J L, Burnett K, *et al.* Processing images in entangled quantum systems [J]. Kluwer Academic Publishers, 2010, 9 (1): 1-11.

[4] Latorre J I. Image compression and entanglement [J]. Computer Science, 2005.

[5] Le P Q, Dong Fangyan, Hirota K. A flexible representation of quantum images for polynomial preparation, image compression, and processing operations [J]. Quantum Information Processing, 2011, 10 (1): 63-84.

[6] Zhang Yi, Lu Kai, Gao Yinghui, *et al.* NEQR: a novel enhanced quantum representation of digital images [J]. Quantum Information Processing, 2013, 12 (8): 2833-2860.

[7] Zhang Yi, Lu Kai, Gao Yinghui, *et al.* A novel quantum representation for log-polar images [J]. Quantum Information Processing, 2013, 12 (9): 3103-3126.

[8] Sang Jianzhi, Wang Shen, Li Qiong. A novel quantum representation of color digital images [J]. Quantum Information Processing, 2017, 16 (2): 42.

[9] Araujo H, Dias J M. An introduction to the log-polar mapping [J]. Workshop on Cybernetic Vision, 1996, 69 (3): 139-144.

[10] Wang Shen, Sang Jianzhi, Song Xianhua, *et al.* Least significant qubit (LSQb) information hiding algorithm for quantum image [J]. Measurement, 2015, 73: 352-359.

[11] 李涛，何煌兴，瞿治国. 一种基于含水印量子图像的自适应量子隐写算法 [J]. 计算机应用研究, 2018, 35 (2): 503-506. (Li Tao, He Huangxing, Qu Zhiguo. Novel self-adaptive quantum steganography algorithm based on quantum image with watermark [J]. Application Research of Computers, 2018, 35 (2): 503-506.)

[12] Heidari S, Farzadnia E. A novel quantum LSB-based steganography method using the Gray code for colored quantum images [J]. Quantum Information Processing, 2017, 16 (10): 242.

[13] Zhang Weiwei, Gao Fei, Liu Bin, *et al.* A quantum watermark protocol [J]. International Journal of Theoretical Physics, 2013, 52 (2): 504-513.

[14] Zhang Weiwei, Gao Fei, Liu Bin, *et al.* A watermark strategy for quantum images based on quantum fourier transform [J]. Quantum Information Processing, 2013, 12 (2): 793-803.

[15] Sang Jianzhi, Wang Shen, Li Qiong. Least significant qubit algorithm for quantum images [J]. Quantum Information Processing, 2016, 15 (11): 1-20.

[16] Qu Zhiguo, Cheng Zhenwen, Luo Mingxing, *et al.* A robust quantum watermark algorithm based on quantum log-polar images [J]. International Journal of Theoretical Physics, 2017, 56 (11): 3460-3476.

[17] Gupta S, Goyal A, Bhushan B. Information hiding using least significant bit steganography and cryptography [J]. International Journal of Modern Education and Computer Science, 2012, 4 (6): 27-34.

[18] Bennett C H, Brassard G. Quantum cryptography: public key distribution and coin tossingIn [C]// Proc of IEEE International Conference on Computers, Systems and Signal processing. 1984: 175-179.